Elliptic Fibers over non-Perfect Residue Fields

Michael Szydlo
RSA Laboratories
Bedford, MA 01730, USA
E-mail: mike@szydlo.com

Version: September 28, 2003

Kodaira and Néron classified and described the geometry of the special fibers of the Néron model of an elliptic curve defined over a discrete valuation ring with a perfect residue field. Tate described an algorithm to determine the special fiber type by manipulating the Weierstrass equation. In the case of non-perfect residue fields, we discover new fiber types which are not on the Kodaira-Néron list. We describe these new types and extend Tate's algorithm to deal with all discrete valuation rings. Specifically, we show how to translate a Weierstrass equation into a form where the reduction type may be easily determined. Having determined the special fiber type, we construct the regular model of the curve with explicit blow-up calculations. We also provide tables that serve as a simple reference for the algorithm and which succinctly summarize the results.

Key Words: Tate's Algorithm, Kodaira symbol, Non-perfect residue field, resolution of singularities, blow-up, elliptic scheme, Néron model, reduction type, discrete valuation ring, flat regular model

1. INTRODUCTION

Useful models of elliptic curves reflect the curve's arithmetic in the geometry of the special fibers. One such model, defined over a discrete valuation ring (DVR), is the Néron model [18]. This model is a flat regular minimal model of an elliptic curve whose fibers contain some information about the structure of the rational points on the curve. The Néron model is defined in terms of a universal mapping property, which makes it automatically a group scheme. Kodaira and Néron classified the possible geometries of the special fibers of these regular schemes. Given a Weierstrass equation defining an elliptic curve over a DVR, Tate presents an algorithm to determine the reduction type of its Néron model. This algorithm may be interpreted as a recipe for the resolution of the singularities on a one-dimensional elliptic scheme. However, both the Kodaira-Néron classification and Tate's algorithm only apply to discrete valuation rings with perfect residue fields.

This paper focuses on the construction of regular elliptic schemes defined over DVRs whose residue field is not perfect. Surprisingly, some of the resulting special fibers are not on the Kodaira-Néron list. We first provide a list of the additional special fiber types, and describe the geometry of each new type. Next, given a Weierstrass equation with coefficients in any DVR, we provide an algorithm to determine which standard or new reduction type it defines, thereby extending Tate's algorithm to allow non-perfect residue fields. As in the classical case, such an algorithm also determines the sequence of blow-ups required to construct the regular model, and the smooth part of these models is still a Néron model.

Elliptic curves are often first considered over number fields, where the residue field associated to each prime ideal is finite and thus perfect. However, it is also natural to consider discrete valuation rings over non-perfect residue fields. For example, to study a one parameter family of elliptic curves defined over $\mathbf{Z}$, one considers an elliptic scheme over the base $\mathbf{Z}[\mathbf{T}]$. Not all localizations of this ring have a perfect residue field[1].

Recently, the new reduction types defined in this paper have been applied to the study of the Grothendieck pairing on the component group of an elliptic curve, in the case of a non-perfect residue field. Bertapelle and Bosch, and Lorenzini[3, 16] have shown that this pairing is not always a perfect pairing, as was previously conjectured[9]. With the new reduction types, Lorenzini produces explicit examples on which Grothendieck's pairing is degenerate. The construction of one-dimensional regular models can also be used as a building block for the construction of flat regular models of elliptic schemes defined over surfaces, or higher dimensional base schemes. This construction, and the material in this article, was the subject of the author's PhD thesis[23]. De-singularizing elliptic threefolds in characteristic 0 was studied earlier by Miranda.[17]

I would like to thank my Ph.D. advisor, Barry Mazur, for guidance on the thesis work, Joe Harris, for teaching me some algebraic geometry, Joe Silverman, for encouraging me to publish this article and for the books that inspired this research, Dino Lorenzini, for his careful reading, Kelly Morgan, for her editorial help, and the anonymous reviewer, for the many detailed comments.

Organization: The rest of this article is organized as follows. In section 2, we present background and notation used throughout the paper, and describe our result. In section 3 we describe the geometry of the new special fiber types. Next, in section 4, we present a series of conditions on the coefficients of a Weierstrass equation which are sufficient to determine the reduction type. These conditions are succinctly presented in several tables. In section 5, we prove that a Weierstrass equation can always be translated to a form satisfying such conditions, thus providing an effective algorithm to determine the reduction type. Finally, in section 6 we discuss how the regular model is constructed using blow-ups, and we carry out the construction for explicit examples which yield new special fiber types. We conclude with suggestions for further related research.

2. BACKGROUND AND NOTATION

Before describing in further detail our results, we present notation and review some background material.

Schemes over a DVR:

Throughout this paper we let R denote a *discrete valuation ring*, and let K be its *field of fractions*. Let m be the unique *maximal ideal* of R, let $\kappa = R/m$ be the *residue field*, and let $\overline{\kappa}$ be an algebraic closure of κ. Let v be the *valuation* on R, and let π be a *uniformizer* for R, so that $v(\pi) = 1$. For every ring we denote its spectrum with $Spec(\cdot)$, and throughout this paper we deal with schemes of finite type over the *base scheme*, $S = Spec(R)$. For each such scheme X/S, we define the *generic fiber* of X to be the variety $X \times Spec(K)$, and the *special fiber* of X to be the variety or scheme $\tilde{X} = X \times Spec(\kappa)$.

For any variety V/K, a scheme X/S is a *model* for V if the generic fiber of X is the variety V. We also call the special fiber $\tilde{X}$ the *reduction* of V in X.

[1] Localizing the ring $\mathbf{Z}[\mathbf{T}]$ at the ideal (T) yields a DVR with perfect residue field $\mathbf{Q}$. Localizing at (2), however, yields a DVR with residue field $\mathbf{F_2}(\mathbf{T})$, which is not perfect.

Elliptic Schemes: To assist the reader in following our explicit calculations, we recall the standard polynomials associated with elliptic curves. First, a *Weierstrass equation* is a cubic equation of the form

$$f = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6) = 0, \tag{1}$$

where $a_i \in K$. We also define the usual quantities $b_2, b_4, b_6, b_8, c_4, c_6$, δ, j:

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6, \tag{2}$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \tag{3}$$

$$c_4 = b_2^2 + 24b_4, \quad c_6 = b_2^3 + 36b_2b_4 - 216b_6, \tag{4}$$

$$\delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \quad j = c_4^3/\delta. \tag{5}$$

We define an *elliptic curve* E/K, to be the subvariety of $\mathbf{P}^2(K)$ which is cut out by a Weierstrass equation with nonzero *discriminant* δ, in the affine neighborhood $Spec(K[x,y])$. Our main object of interest, however, is two-dimensional.

DEFINITION 1. An *Elliptic Scheme*, C/R, is a two-dimensional projective scheme flat over $Spec(R)$ whose generic fiber is an elliptic curve E/K. For each Weierstrass equation $f = 0$ with coefficients in R, $(f \in R[x,y], \delta \neq 0)$, we define the *Elliptic Scheme defined by* f to be the closure of $Spec(R[x,y]/(f))$ in $\mathbf{P}^2(S)$.

We denote the special fiber of an elliptic scheme by $\tilde{C} = C \otimes_R \tilde{\kappa}$, and the *geometric special fiber* by $\overline{C} = C \otimes_R \overline{\kappa}$.

Regular Models: Recall that a local ring of dimension d with maximal ideal m_p is a *regular local ring* if $dim(m_p/m_p^2) = d$. A scheme S is then called *regular* or *non-singular* if for every point $p \in S$, the local ring O_p is regular. If O_p is not regular, S is said to have a *singularity* at p.

We consider the regularity of several objects: (1) the special fiber $\tilde{C}$, (2) the geometric special fiber $\overline{C}$, and (3) C itself, which is a two-dimensional scheme. The geometric special fiber $\overline{C}$ of an elliptic scheme defined by the Weierstrass equation $f = 0$ is singular if and only if $v(\delta) > 0$, in which case the singularity is either a node or a cusp. A more general elliptic scheme C, defined with several coordinate patches, can be more complicated. Considering an affine coordinate patch of the form $Spec(R[x,y]/(g))$, (where $g \in R[x,y]$) [2], the singular points $p \in \overline{C}$, are those for which both $\frac{df}{dx} = 0$ and $\frac{df}{dy} = 0$, (mod π). Such a singular point in $\overline{C}$ may, or may not, be κ-rational, and if not, its image under the map $\overline{C} \to \tilde{C}$ can be a regular point of $\tilde{C}$. Finally, a singular point $\tilde{p} \in \tilde{C}$, may or may not be a singular point of (the surface) C. This can be tested directly from the definition: it is singular if $dim(m_p/m_p^2) > 2$.

The regular models we construct will also be *proper*, *flat*, and *minimal*. Assuming that κ is perfect, the *smooth* part of a regular, proper, minimal model of an elliptic curve E/K is the *Néron model* of the curve, and in particular, a *group scheme*. We refer the reader to [6, 8, 10, 22] for a definition and discussion of these terms.

Minimal Weierstrass Equations: An *R-translation* of a Weierstrass Equation is an R-linear change of variables of the form $x \mapsto x' + \alpha$, $y \mapsto y' + \beta x' + \gamma$, where α, β, $\gamma \in R$. See [21] for the formulas explaining how the Weierstrass coefficients a_i change under an R-translation.

[2] This is an example. Not every coordinate patch must be in such a form.

Definition 2. A Weierstrass Equation $f \in R[x, y]$ is *Minimal* if there is no R-translation for which the translated coefficients a_i' satisfy $\pi^i | a_i'$ for $i \in \{1, 2, 3, 4, 6\}$.

A minimal Weierstrass equation can be used to construct a *minimal model*. See [10, 22] for a description of the relationship between a minimal Weierstrass equation and a minimal model.

Kodaira-Néron Special Fibers: We now define some terms to describe the geometry of the special fibers, and review Kodaira's notation for standard reduction types.

The special fiber is neither required to be irreducible nor reduced, so we define the *components* of a curve over κ or $\overline{\kappa}$ to be the maximal irreducible subschemes. A component is a *rational curve* if its reduced subscheme, L, is isomorphic to $\mathbf{P}^1/\kappa$. The *multiplicity* of a rational curve locally defined by a polynomial f is the valuation of f in the local ring O_L (which is a DVR). When two distinct components meet at a point p, the intersection defines a zero dimensional scheme supported at p. The degree of this scheme is called the *local intersection multiplicity* of the components at p. Two components intersect *transversally* at a point if the intersection multiplicity is one.

Kodaira and Néron classified the special fibers into *reduction types* according to the geometry (genus and regularity) of the reduced components, the multiplicity of each component, and the local intersection multiplicity between pairs of components. The following table presents the *Kodaira symbol* of each type, and the number of components (when κ is algebraically closed). Note that the symbols I_n, and I_n^* actually denote a family of reduction types, one for each integer $n \geq 1$.

I_0	I_n	II	III	IV	I_0^*	I_n^*	IV^*	III^*	II^*
1	n	1	2	3	5	5+n	7	8	9

(6)

The familiar types I_0, I_1, and II each consist of only a single component, namely an elliptic curve, a nodal cubic, and a cuspidal cubic. Type III has two components meeting tangentially, and each remaining type consists of two or more rational curves which intersect transversally. For further description of these types, including the configuration and multiplicity of the components, we refer the reader to [13, 18, 22].

Lastly, we remark that when κ is not algebraically closed, one or more of the components in the geometric special fiber $\overline{C}$ may be identified in $\tilde{C}$.

Blow-ups: It is conjectured that every scheme is birational to a regular scheme, but this has only been proved for certain classes of schemes[1, 11, 12], including the arithmetic surfaces C/R considered in this paper. The construction of a regular model of a scheme is called a *resolution of singularities*. Given that the general resolution of singularities is still open, it is not obvious that general elliptic schemes always have regular models.

One technique to create a regular model is to use the *blow-up* construction. For each subscheme T of S the *blow-up of S along T* is a scheme S' with a birational morphism $S' \to S$, which is an isomorphism outside of T. When $S = Spec(R)$ is affine, and $\{g_i \in R\}$, cut out T, the $\{g_i\}$ naturally define a rational map $S \to \mathbf{P}^k(R)$. In this case we can define the blow-up of S along T to be the closure of the graph of ϕ in $S \times_R \mathbf{P}^k(R)$. In practice, one describes the blow-up scheme in terms of the $k + 1$ standard affine coordinate neighborhoods of $S \times_R \mathbf{P}^k(R)$, effectively performing a substitution of variables in each neighborhood. See [7, 8, 10, 22] for several different, but equivalent, complete definitions of a blow-up which apply to more general schemes $T \subset S$.

By repeating this blow-up construction for wisely chosen subschemes T containing the singular points, one hopes to obtain a regular scheme S'' and a birational morphism $S'' \to S$.

Tate's algorithm: It is known that when κ is perfect, a flat proper regular minimal model of an elliptic curve always exists. Tate's algorithm is a procedure used to determine the special fiber type of such a good model, when it is defined by a minimal Weierstrass equation[3].

The constructive version of Tate's algorithm uses the blow-up construction to resolve the singularities on the elliptic scheme $SpecR[x, y]/(f)$, defined by the Weierstrass equation $f = 0$.

At each stage of the algorithm, the scheme is checked for regularity, and if still singular, it is replaced with the blow-up along a certain subscheme T.The resulting scheme, defined locally in multiple coordinate patches, is the regular model sought. Tate conveniently chose to translate the coordinates of the Weierstrass equation in the successive stages of his algorithm, so that the existence and location of the singularities could easily be determined by examining the valuations of the a_i, or b_i.

The non-constructive version of Tate's algorithm skips the actual blow-up computations, but only explains how to translate the coordinates of the original Weierstrass equation so that the required sequence of blow-ups, and therefore the reduction type, can be determined directly from the valuations of the a_i (or of the quantities $b_2, b_4, b_6, b_8, c_4, c_6$, and δ).

Our results: We have extended Tate's algorithm to the case when κ is not perfect. We posed the question:

"Do the blow-ups in Tate's algorithm still produce a regular model?"

We found that they often do, but not always. When they do not, we discovered new special fiber types in the regular minimal model.

The first result is that only finitely many new reduction types (and families of reduction types) that arise. In other words, with a few modifications, this sequence of blow-ups still always terminates, and produces a regular scheme. We list and describe these new reduction types.

Secondly, we produce a series of tables which help to concisely summarize this extention of Tate's algorithm. For every reduction type, we record the form of the Weierstrass equation, after it has been translated, thus producing sufficient conditions on the $\{a_i\}$ for each type.

Next, we present a simple, effective procedure to translate any Weierstrass equation into such a form, thus completing the determination of the special fiber when κ is not perfect.

Lastly, we return to the construction of the regular model, and compare the required sequence of blow-ups to those specified in Tate's original algorithm. By verifying the regularity of each kind of resulting scheme, we have a proof that our extention of Tate's algorithm correctly determines the reduction type.

[3]When κ is perfect, and $char(\kappa) \neq 2, 3$, it is well known that the reduction type can be easily determined by examining δ, and j.

3. A DESCRIPTION OF THE NEW REDUCTION TYPES

In this section, we list and describe the new special fiber types. To complement the standard Kodaira symbols listed above in (6), we now introduce some new symbols for the extra reduction types, and record the number of components of each in $\overline{C}$. Note that the symbols K_n, K'_n, and T_n each denote a family of reduction types, indexed by $n \in \mathbf{Z}, n \geq 1$.

Z_1	Z_2	X_1	X_2	Y_1	Y_2	Y_3	K_{2n}	K'_{2n}	K_{2n+1}	T_n
1	3	1	4	1	2	5	$n+1$	$n+1$	$n+1$	$n+4$

(7)

We are now going to describe the geometry of these curves $\tilde{C}/\kappa$. We do this by first describing the geometric special fibers $\overline{C}/\overline{\kappa}$, and then describing the behavior of the singular points or curves under the mapping $\rho : \overline{C} \rightarrow \tilde{C}$.

If p is a point in $\overline{C}$, and $\tilde{p} = \rho(p)$ is its image in $\tilde{C}$, we say that $\rho(p)$, *ramifies* in $\overline{C}$ to a multiplicity k point if $\rho^{-1}(\tilde{p})$ has multiplicity $k > 1$. We use the same terminology for a curve $\tilde{p} \in \tilde{C}$. Often, singular points in $\overline{C}$ become regular points in $\tilde{C}$. We also define the *smooth locus* of points in $\tilde{C}$ to be the open subscheme containing only points whose inverse image in $\overline{C}$ is reduced and non-singular.

3.1. New Types with Residue Characteristic 3

When $char(\kappa) = 3$, the special fiber is either a standard Kodaira type listed above in list (6), or one of the two new types, Z_1, or Z_2.

• **Type $\mathbf{Z_1}$:** Geometrically, type Z_1 is a cubic curve with a cusp $p \in \overline{C}$, which is not κ-rational. Its image, $\rho(p) \in \tilde{C}$, is a regular point which ramifies in a degree three extention of κ (Fig. 1).

• **Type $\mathbf{Z_2}$:** Geometrically, type Z_2 consists of a chain of three rational curves, intersecting transversally, of multiplicity 1, 2, and 3. The first two curves are κ-rational, and the last, p, is not. Its image, $\rho(p) \in \tilde{C}$, is generically regular, and it ramifies in a degree three extention of κ (Fig. 2).

FIG. 1 Types X_1, Y_1, and Z_1

3.2. New Types with Residue Characteristic 2

When $char(\kappa) = 2$, the special fiber is either a standard Kodaira type listed above (6), or any one of the new types, except Z_1, or Z_2.

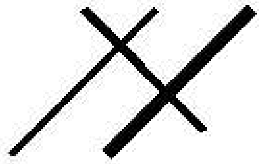

FIG. 2 Type Z_2

• **Type $\mathbf{X_1}$:** Geometrically, type X_1 is a cubic curve with a cusp $p \in \overline{C}$, which is not κ-rational. Its image, $\rho(p) \in \tilde{C}$, is a regular point which ramifies in an extention of κ of degree two or four[4] (Fig. 1).

• **Type $\mathbf{X_2}$:** Geometrically, type X_2 consists of four rational curves, intersecting transversally, as follows. A first κ-rational curve of multiplicity 2, meets two rational curves of multiplicity 1, and a second curve of multiplicity 2. This last curve, p, is not κ-rational. Its image, $\rho(p) \in \tilde{C}$, is generically regular, and ramifies in a degree two extention of κ (Fig. 3).

• **Type $\mathbf{Y_1}$:** Type Y_1 is geometrically a cubic curve with a cusp $p \in \overline{C}$, which is not κ-rational. Its image, $\rho(p) \in \tilde{C}$, is a regular point which ramifies in an extention of κ of degree two (Fig. 1).

• **Type $\mathbf{Y_2}$:** Geometrically, type Y_2 consists of two rational curves of multiplicity 1 and 2, intersecting transversally. The second curve, p, is not κ-rational. Its image, $\rho(p) \in \tilde{C}$, is generically regular, and ramifies in a degree two extention of κ (Fig. 4).

• **Type $\mathbf{Y_3}$:** Geometrically, type Y_3 consists of a chain of five rational curves of multiplicity 1, 2, 3, 4 and 2, intersecting transversally. The first three curves are κ-rational, but the last two, p and p' are not. The image of the first, $\rho(p) \in \tilde{C}$ is of multiplicity 2 over κ, and thus everywhere singular. The image of the second, $\rho(p') \in \tilde{C}$, is generically regular. Both of $\rho(p)$ and $\rho(p')$ ramify in a degree two extention of κ (Fig. 4).

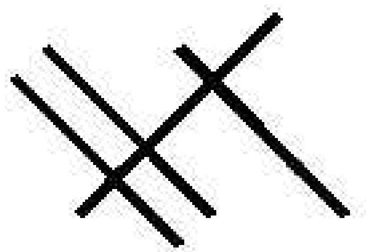

FIG. 3 Type X_2

• **Types $\mathbf{K_n}$ (n odd):** Geometrically, the types K_n for odd $n > 1$ consist of a chain of one rational curve, and $\frac{n-1}{2}$ multiplicity 2 curves, which intersect transversally. Each multiplicity 2 component is not κ-rational, but has a regular image in $\tilde{C}$ which ramifies in a degree two extention of κ (Fig. 5). Type K_1 consists

[4]The degree depends on the field in which both coordinates of the cusp are rational.

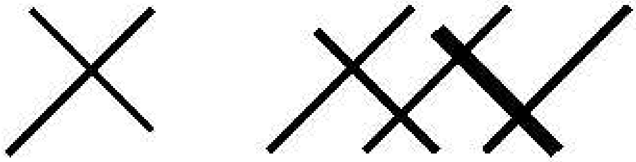

FIG. 4 Types Y_2 and Y_3

of a single component, a cuspidal cubic with a rational cusp. (It is identical to type **II**).

• **Types $\mathbf{K_n}$ (n even):** Geometrically, the types K_n for even $n > 2$ have the same configuration as the types K_n for odd n, except there are $\frac{n-2}{2}$ multiplicity 2 components and an additional rational curve intersecting the last multiplicity 2 component transversally (Fig. 5). Type K_2 consists of two rational curves meeting tangentially at a point. (It is identical to type **III**).

• **Types $\mathbf{K'_n}$ (n even):** Geometrically, the types K'_n for even n have the same configuration as the types K_n for odd n, except there are $\frac{n}{2}$ multiplicity 2 components. The last component contains no κ-rational point, except the point at which it intersects the previous component (Fig. 5).

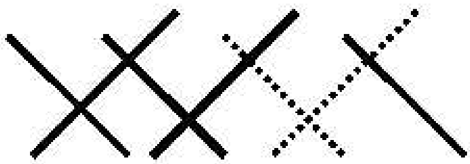

FIG. 5 Types K_n ($n \in Z$, $n > 0$), and types K'_n, ($n \in 2Z$, $n > 0$)

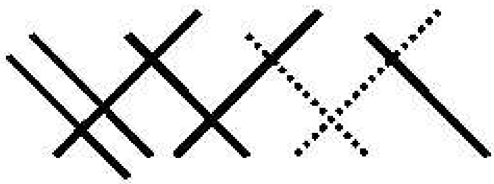

FIG. 6 Type T_n ($n \in Z$, $n > 0$)

• **Types $\mathbf{T_n}$ ($n > 0$):** Geometrically, the types T_n consist of two rational curves meeting the first component of a chain of $\frac{n-1}{2}$ multiplicity 2 curves, all intersecting transversally. All components are κ-rational, except the last one, p. Its image, $\rho(p) \in \tilde{C}$, is generically regular, and ramifies in a degree two extention of κ (Fig. 6).

Having defined and described these new special fiber types, we now assert that this list is complete.

THEOREM 3.1 (Reduction Types). *Let C/R be a flat proper regular minimal model of E/K. Then the special fiber, $\tilde{C}$, is either a standard reduction type in Kodiara's list (6), or one of the new reduction types in the list (7), and defined in this section.*

The proof of Theorem 3.1 will be completed later, in section 6 when we will have constructed the regular model of the elliptic curve defined by any Weierstrass equation.

4. VALUATIONS OF WEIERSTRASS COEFFICIENTS

In this section we associate a set of conditions on the Weierstrass coefficients to each reduction type. Although not every Weierstrass equation meets such criteria, at least these conditions are sufficient to determine the reduction type.

The conditions are succinctly presented in several tables, where each column corresponds to a different reduction type. When κ is perfect, such conditions can be expressed completely in terms of the valuations of the Weierstrass coefficients. In general, however, other kinds of conditions will be required, and we list them here.

1. $v(\phi) = a$, for $\phi \in \{a_1, a_2, a_3, a_4, a_6, b_2, b_4, b_6, b_8, c_4, c_6, \delta\}$.
2. $v(\phi) \geq a$, for $\phi \in \{a_1, a_2, a_3, a_4, a_6, b_2, b_4, b_6, b_8, c_4, c_6, \delta\}$.
3. The reduction $\frac{a_i}{\pi^a} \pmod{\pi}$ is not a square in κ.
4. The reduction $\frac{a_i}{\pi^a} \pmod{\pi}$ is not a cube in κ.
5. A specified auxiliary polynomial has distinct roots, or not.
6. A specified auxiliary curve, f', contains no κ-rational points.

Table Notations: These six kinds of conditions are described with entries in a table, as follows. Fixing a reduction type, the entry in the row labeled $v(\phi)$ represents one condition, according to the following notation. An integer a means $v(\phi) = a$. The symbol a^+ means $v(\phi) \geq a$. The symbol a^{ns} denotes the condition that $\phi/\pi^a \pmod{\pi}$ is not a square. Similarly, the symbol a^{nq} denotes the condition that $\phi/\pi^a \pmod{\pi}$ is not a cube. The symbol a^{nt} denotes the condition that the quadratic polynomial $Y^2 = a_2X^2 + \frac{a_6}{\pi^a}$ contains no κ-rational points. We define the element d_F to be $a_2a_4 - a_6$; its valuation determines whether or not the auxiliary polynomial (13) has distinct roots.

We present the tables of conditions according the the characteristic of κ, starting with $char(\kappa) = 0$ or $char(\kappa) \geq 5$.

4.1. Char $\neq 2, 3$, General Form

Not surprisingly, when $char(\kappa) \neq 2, 3$, any set of conditions which suffice to determine the reduction type when κ is perfect are also sufficient when κ is not perfect. In particular, this implies that when $char(\kappa) \neq 2, 3$, none of the new reduction types appear as the special fiber of a regular model, and additionally, the reduction type may be still be determined from $v(\delta)$, and $v(j)$ alone.

With this in mind, we still choose to present general conditions on the Weierstrass coefficients without completing the square and assuming that $a_1 = a_3 = 0$. This way the data contained in the following tables serves as the base case which

TABLE 1
Standard Kodaira types for Tate's algorithm ($char(\kappa) \neq 2, 3$).

Type	I_0	I_n	II	III	IV	I_0^*	I_n^*	IV^*	III^*	II^*	o/w
$v(a_1)$		0^+	1^+	1^+	1^+	1^+	1^+	1^+	1^+	1^+	1^+
$v(a_2)$		0^+	1^+	1^+	1^+	1^+	1	2^+	2^+	2^+	2^+
$v(a_3)$		1^+	1^+	1^+	1^+	2^+	2^+	2^+	3^+	3^+	3^+
$v(a_4)$		1^+	1^+	1	2^+	2^+	3^+	3^+	3	4^+	4^+
$v(a_6)$		1^+	1	2^+	2^+	3^+	4^+	4^+	5^+	5	6^+
$v(b_2)$		0					1				
$v(b_4)$				1					3		
$v(b_6)$			1		2			4		5	
$v(c_4)$		0		1		2			3		
$v(c_6)$			1		2	3		4		5	
$v(d)$	0	n	2	3	4	6	7^+	8	9	10	12^+

will highlight the differences that appear later, when $char(\kappa) = 2$ or 3. These conditions are also a good reference when constructing the models with blow-ups, and are useful when resolving the singularities of elliptic schemes over higher dimensional bases[5] [23].

Certain of the conditions in Table 1 have equivalent formulations in terms of the number of roots of certain auxiliary polynomials. For example, the condition $v(b_6) = 4$ which applies to type IV, is equivalent to specifying that the polynomial

$$X^2 + \frac{a_3}{\pi} X + \frac{a_6}{\pi^2} \tag{8}$$

has distinct roots in $\overline{\kappa}$. The condition $v(b_6) = 8$ which applies to type IV^*, is equivalent to specifying that

$$X^2 + \frac{a_3}{\pi^2} X + \frac{a_6}{\pi^4} \tag{9}$$

has distinct roots in $\overline{\kappa}$. Finally, the condition $v(c_6) = 3$ is equivalent to the condition that

$$X^3 + \frac{a_2}{\pi} X^2 + \frac{a_4}{\pi^2} X + \frac{a_6}{\pi^3} \tag{10}$$

has three distinct roots in $\overline{\kappa}$.

4.2. The Families I_n and I_n^*

If Table 1 implies that the reduction type is in the family I_n, the conditions in Table 2 can be used to determine the exact reduction type. Similarly, if a reduction type is in the family I_n^*, Table 3 can be used to determine the exact type.

As before, certain conditions in Table 3 may be formulated in terms of the number of roots of certain auxiliary polynomials. When k is odd, the condition $v(b_8) = k$ implies that the polynomial

$$X^2 + \frac{a_3}{\pi^{\frac{k-1}{2}}} X + \frac{a_6}{\pi^{k-1}} \tag{11}$$

[5] One approach applies Tate's algorithm to an equation defined over a DVR which may have characteristic zero, yet arises as the localization of a two dimensional ring in which 2 is not a unit.

TABLE 2
Reduction types in the family I_n.

Type	I_1	I_2	I_3	I_4	I_5	$\cdots$
$v(a_1)$	0^+	0^+	0^+	0^+	0^+	$\cdots$
$v(a_2)$	0^+	0^+	0^+	0^+	0^+	$\cdots$
$v(a_3)$	1^+	1^+	2^+	2^+	2^+	$\cdots$
$v(a_4)$	1^+	1^+	2^+	2^+	2^+	$\cdots$
$v(a_6)$	1	2^+	3	4^+	5	$\cdots$
$v(b_2)$	0	0	0	0	0	$\cdots$
$v(b_8)$	1	2	3	4	5	$\cdots$
$v(d)$	1	2	3	4	5	$\cdots$

TABLE 3
Reduction types in the family I_n^*, ($char(\kappa) \neq 2$).

Type	I_1^*	I_2^*	I_3^*	I_4^*	I_5^*	$\cdots$
$v(a_1)$	1^+	1^+	1^+	1^+	1^+	$\cdots$
$v(a_2)$	1	1	1	1	1	$\cdots$
$v(a_3)$	2^+	3^+	3^+	4^+	4^+	$\cdots$
$v(a_4)$	3^+	3^+	4^+	4^+	5^+	$\cdots$
$v(a_6)$	4^+	5^+	6^+	7^+	8^+	$\cdots$
$v(b_8)$	5	6	7	8	9	$\cdots$
$v(d)$	7	8	9	10	11	$\cdots$

has distinct roots in $\overline{\kappa}$. If k is even, the polynomial

$$\frac{a_2}{\pi}X^2 + \frac{a_4}{\pi^{\frac{k}{2}}}X + \frac{a_6}{\pi^{k-1}} \tag{12}$$

has distinct roots in $\overline{\kappa}$. These facts will be useful to the reader who wishes to calculate the blow-ups for the types in Table 3.

Interestingly, Table 2 turns out to apply in all residue characteristics, and Table 3 still applies when $char(\kappa) = 3$.

4.3. Char 3 Residue Field

Here we treat the case where $char(\kappa) = 3$, and define the conditions on the Weierstrass coefficients in Table 4. Notice the appearance of a new kind of condition which is not needed when $char(\kappa) \neq 2, 3$. Namely, one of the conditions for the new type Z_1 is that $a_6 \pmod{\pi}$ is not a cube in κ. Similarly, one of the conditions for the new type Z_2 is that $a_6/\pi^3 \pmod{\pi}$ is not a cube in κ. Recall that we use the notation 0^{nq} and 3^{nq}, for these new kinds of conditions in Table 4.

There are no new kinds of conditions appearing in the families I_n and I_n^* when $char(\kappa) = 3$. If Table 4 implies that the reduction type is in one of these families, the same tables presented above, Table 2 and Table 3, may be used to determine the exact type.

TABLE 4
Characteristic 3 Reduction Types

Type	I_0	I_n	Z_1	II	III	IV	I_0^*	Z_2	I_n^*	IV^*	III^*	II^*	o/w
$v(a_2)$		0	1^+	1^+	1^+	1^+	1^+	2^+	1	2^+	2^+	2^+	2^+
$v(a_4)$		1^+	1^+	1^+	1	2^+	2^+	3^+	3^+	3^+	3	4^+	4^+
$v(a_6)$		1^+	0^{nq}	1	2^+	2	3^+	3^{nq}	4^+	4	5^+	5	6^+
$v(d)$	0	n	1^+	2^+	3	4^+	6	7^+	7^+	8^+	9	10^+	12^+

TABLE 5
Characteristic 2 Reduction Types

Type	I_0	I_n	X_1	Y_1	K_n	II	III	IV	Y_2	I_0^*	X_2	I_n^*	IV^*	Y_3	III^*	II^*	o/w
$v(a_1)$	0^+	0	1^+	1^+	1^+	1^+	1^+	1^+	1^+	1^+	1^+	1^+	1^+	1^+	1^+	1^+	1^+
$v(a_2)$	0^+	0^+	0^+	0^+	0^{ns}	1^+	1^+	1^+	1^+	1^+	2^+	1	2^+	2^+	2^+	2^+	2^+
$v(a_3)$	0^+	1^+	1^+	1^+	1^+	1^+	1^+	1	2^+	2^+	2^+	2^+	2	3^+	3^+	3^+	3^+
$v(a_4)$	0^+	1^+	0^{ns}	1^+	1^+	1^+	1	2^+	2^+	2^+	2^{ns}	3^+	3^+	3^+	3	4^+	4^+
$v(a_6)$	0^+	1^+	0^+	0^{ns}	1^+	1	2^+	2^+	2^{ns}	3^+	4^+	4^+	4^+	4^{ns}	5^+	5	6^+
$v(d_F)$	0									3							
$v(d)$	0							4					8				12^+

4.4. Char 2 Residue Field

The case where $char(\kappa) = 2$ is the most interesting one. We define the conditions on the Weierstrass equations in Table 5 associated to each reduction type. We see several new kinds of condition in characteristic two. First, for each of the new reduction types X_1, Y_1, X_2, Y_2, Y_3, and for each of the new types in the family K_n, one of the conditions is that a certain element is not a square in κ. Recall that in Table 5 the notation a^{ns} means that $a_i/\pi^a \pmod{\pi}$ is not a square in κ.

A second new kind of condition is present for types I_0^*. The auxiliary polynomial

$$F = X^3 + \frac{a_2}{\pi}X^2 + \frac{a_4}{\pi^2}X + \frac{a_6}{\pi^3} \tag{13}$$

must have distinct roots for type I_0^*. We define $d_F = a_2a_4 - a_6$, the discriminant of this polynomial (mod π), so that we may succinctly denote this condition by $v(d_F) = 3$ in Table 5. Note that the conditions defined in this table imply that for type X_2 the polynomial (13) has a double root which is not κ-rational.

Reading The Table. Table 5 contains the most complex set of conditions on the Weierstrass equation, so let us give an example of how to read the table columns. Let $f = 0$, $f \in R[x, y]$ be a Weierstrass equation. According to the first column, f is of type I_0 if $v(d) = 0$. According to the second column, f belongs to a type in the I_n family if $v(a_1) = 0$, $v(a_2) \geq 0$, $v(a_3) \geq 1$, $v(a_4) \geq 1$, and $v(a_6) \geq 1$, and we consult Table 2 to determine exactly which type it is. The third column tells us that f is of type X_1 if $v(a_1) \geq 1$, $v(a_2) \geq 0$, $v(a_3) \geq 1$, $v(a_4) = 0$, $v(a_6) \geq 0$, and a_4 is not a square in κ. Similarly, Table 5 defines conditions for the other reduction types.

Consulting subcharts. Notice that Table 5 contains conditions for the three infinite families I_n, K_n, and I_n^*. If this table implies that the reduction type is in

TABLE 6
Reduction types in the family K_n.

Type	K_1	K_2	K_2'	K_3	K_4	K_4'	K_5	K_6	K_6'	$\cdots$
$v(a_1)$	1^+	1^+	1^+	1^+	1^+	1^+	1^+	1^+	1^+	$\cdots$
$v(a_2)$	0^{ns}	0^{ns}	0^{ns}	0^{ns}	0^{ns}	0^{ns}	0^{ns}	0^{ns}	0^{ns}	$\cdots$
$v(a_3)$	1^+	1^+	2^+	2^+	2^+	2^+	3^+	3^+	4^+	$\cdots$
$v(a_4)$	1^+	1^+	2^+	2^+	2^+	2^+	3^+	3^+	4^+	$\cdots$
$v(a_6)$	1	2^+	2^{nt}	3	4^+	4^{nt}	5	6^+	6^{nt}	$\cdots$
$v(b_8)$		2			4			6		$\cdots$

one of these families, a sub-table must be consulted to determine the exact type. For the family I_n, the conditions in Table 2 can be used to determine the exact type. For the family K_n, Table 6, presented below, must be consulted. Finally, for the family I_n^*, the conditions in Table 7, also presented below, can be used to determine the exact type.

4.5. Char 2 K_n Detail

The family of reduction types K_n is a sequence of new reduction types which appear only when $char(\kappa) = 2$. Each type in this family has the common condition that $a_2 \pmod{\pi}$ is not a square in κ. Table 6 presents the conditions sufficient to determine each reduction type in this family. Note that a new kind of condition, denoted a^{nt}, is used for the types K_n', (n even). Recall that this condition has been defined to mean that the quadratic curve in $\kappa[X, Y]$

$$Y^2 = a_2 X^2 + \frac{a_6}{\pi^n} \tag{14}$$

contains no κ-rational points. The notation a^{nt} was chosen because there is no κ-rational point that can be translated.

4.6. Char 2 I_n^* Detail

The subfamily I_n^* for $char(\kappa) = 2$, differs from the usual subfamily I_n^* when $char(\kappa) \neq 2$. Here, the family I_n^* also includes the new types T_n, for $n > 0$. In Table 7, we present the conditions on the Weierstrass equations sufficient to determine the type. Notice the conditions for the types T_n: for n odd we require that $\frac{a_6}{\pi^{n+3}}$ not be a square in κ, and for n even we require that $\frac{a_6}{a_2 \pi^{n+2}}$ not be a square in κ.

4.7. Translated Form Definitions

Having specified a set of conditions associated to each reduction type, we now make a formal definition.

DEFINITION 3. Let R be an arbitrary DVR with residue field κ, and let $f \in R[x, y]$ define a Weierstrass equation. We say that the polynomial f, and the Weierstrass equation $f = 0$ is in *Translated Form* if one of the following holds:

- $char(\kappa) \neq 2, 3$, and f meets all conditions for a type in Table 1.

TABLE 7
Reduction types in the family I_n^*.

Type	I_1^*	T_1	I_2^*	T_2	I_3^*	T_3	I_4^*	T_4	$\cdots$
$v(a_1)$	1^+	1^+	1^+	1^+	1^+	1^+	1^+	1^+	$\cdots$
$v(a_2)$	1	1	1	1	1	1	1	1	$\cdots$
$v(a_3)$	2	3^+	3^+	3^+	3	4^+	4^+	4^+	$\cdots$
$v(a_4)$	3^+	3^+	3	4^+	4^+	4^+	4	5^+	$\cdots$
$v(a_6)$	4^+	4^{ns}	5^+	5	6^+	6	7^+	7	$\cdots$
$v(a_6/a_2)$				4^{ns}				6^{ns}	$\cdots$
$v(b_8)$	5	6^+	6	7^+	7	8^+	8	9^+	$\cdots$

- for any κ, f meets all conditions for a type in Table 2.
- $char(\kappa) \neq 2$, and f meets all conditions for a type in Table 3.
- $char(\kappa) = 3$, and f meets all conditions for a type in Table 4.
- $char(\kappa) = 2$, and f meets all conditions for a type in Table 5.
- $char(\kappa) = 2$, and f meets all conditions for a type in Table 6.
- $char(\kappa) = 2$, and f meets all conditions for a type in Table 7.

This concludes the presentation of the tables of conditions, and the definition of what it means for a Weierstrass equation to be in translated form. We next discuss what to do with Weierstrass equations which are not in translated form.

5. TRANSLATING THE WEIERSTRASS EQUATION

In this section we prove that every Weierstrass equation may be put into translated form.

THEOREM 5.1. *Let R be an arbitrary DVR with residue field κ. Let f be a minimal Weierstrass equation with coefficients in R. There always exist R translations $x \mapsto x' + \alpha$ and $y \mapsto y' + \beta x + \gamma$ such that the modified Weierstrass equation is in translated form.*

There is an effective algorithm to compute these R-translations.

Because we will prove that the conditions presented in section 4 determine the reduction type, the translations of Theorem 5.1 constitute the extention of Tate's algorithm to general DVRs. There are several components of the algorithm, each corresponding to a table in section 4: There is one main procedure for each of the cases:

- $char(\kappa) \neq 2, 3$.
- $char(\kappa) = 3$.
- $char(\kappa) = 2$.

There is also a secondary procedure for each of the four infinite families:

- I_n.
- I_n^* ($char(\kappa) \neq 2$).
- I_n^* ($char(\kappa) = 2$).
- K_n.

These procedures all follow a common paradigm, which we briefly discuss. In each procedure, a Weierstrass equation is compared to the conditions described in the columns of the table, until it successfully meets such a set of conditions. These tests proceed in order of the columns (from left to right), and if a test fails, a translation may be made before moving to the next column. So, to fully describe each procedure, we simply need to specify which, if any, translations are to be made when the conditions of a column are not met. If the conditions defined in the rightmost columns of Tables 1, 4, or 5 are met, then we begin anew with a more minimal Weierstrass equation.

Once the table of conditions is known, it is not difficult to recover the details of the translations required to complete the definition of of each procedure. When $char(\kappa) \neq 2, 3$, these translations are identical to those in Tate's original algorithm. We will provide details for the main procedure when $char(\kappa) = 2$, and also for the secondary procedure for the family K_n. These are the two most interesting procedures, and we leave the rest for the reader to discover, or find in [23].

5.1. Char(κ) = 2 Main Procedure

Let f be a Weierstrass equation with coefficients in R. The following 17 step procedure will produce an R translation $x \mapsto x' + \alpha$ and $y \mapsto y' + \beta x' + \gamma$ such that the revised coefficients $\{a_i\}$ satisfy the conditions of one of the types (or families of types) in Table 5. The reader can most easily verify this proof by following along with Table 5, sequentially examining the conditions and possible translations.

1. First suppose $v(d) = 0$. Then we have type $\boxed{I_0}$.

2. Suppose instead $v(d) > 0$ and $v(a_1) = 0$. Translate via $x = x' - a_3/a_1$ and compute new $\{a_i\}$. Then $v(a_3) > 0$. The singularity at (x, y) on the special fiber satisfies $\frac{df}{dy} = 2y_0 + a_1 x_0 + a_3 = 0 \pmod{\pi}$. So now $x = 0$ at the singular point. Now translate via $y = y' + a_4/a_1$, and compute new $\{a_i\}$. Now $v(a_4) > 0$. The singularity at (x_0, y_0) on the special fiber satisfies $\frac{df}{dx} = a_1 y_0 + a_4 = 0 \pmod{\pi}$. So y=0 at the singular point as well. Next, the fact that $f(x_0, y_0) = 0 \pmod{\pi}$ implies that $v(a_6) > 0$. So, collecting these conditions, $v(a_1) = 0$, $v(a_3) > 0$, $v(a_4) > 0$, and $v(a_6) > 0$, we are in one of the cases $\boxed{I_n}$. We then consult Table 2 to determine exactly which type it is.

3. Now suppose both $v(d) > 0$ and $v(a_1) > 0$. Then the condition $\frac{df}{dy} = 0 \pmod{\pi}$ at the singular point (x_0, y_0) implies $2y_0 + a_1 x_0 + a_3 = a_3 = 0 \pmod{\pi}$. So $v(a_3) > 0$. Assume additionally that a_4 is not a square in κ. Then we are in the case $\boxed{X_1}$.

4. If instead a_4 is a square in κ, translate via $x = x' + \alpha$ where $\alpha^2 = a_4 \pmod{\pi}$ and compute new $\{a_i\}$. Now $v(a_4) > 0$. If a_6 is not a square in κ, we are in the case $\boxed{Y_1}$.

5. If instead a_6 is a square in κ, translate via $y = y' + \alpha$ where $\alpha^2 = a_6 \pmod{\pi}$ and compute new $\{a_i\}$. Now $v(a_6) > 0$. Assume that a_2 is not a square in κ. Then we are in one of the cases $\boxed{K_n}$, or $\boxed{K'_n}$. We then consult Table 6 to determine exactly which type it is.

6. If instead a_2 is a square in κ, translate via $y = y' + \beta x$ where $\beta^2 = a_2 \pmod{\pi}$ and compute new $\{a_i\}$. Now $v(a_2) > 0$. These cumulative translations imply $v(a_1) \geq 1$, $v(a_2) \geq 1$, $v(a_3) \geq 1$, $v(a_4) \geq 1$, and $v(a_6) \geq 1$. Suppose that additionally $v(a_6) = 1$. Then we are in the case $\boxed{II}$.

7. Suppose instead $v(a_6) \geq 2$, and additionally $v(a_4) = 1$. Then we are in the case $\boxed{III}$.

8. Suppose instead $v(a_4) \geq 2$, and additionally $v(a_3) = 1$. Then we are in the case $\boxed{IV}$.

9. Suppose instead $v(a_3) \geq 2$, and additionally $\frac{a_6}{\pi^2}$ is not a square in κ. Then we are in the case $\boxed{Y_2}$.

10. If instead $\frac{a_6}{\pi^2}$ is a square in κ, translate via $y = y' + \alpha$ where $\alpha^2 = \frac{a_6}{\pi^2} \pmod{\pi}$ and compute new $\{a_i\}$. Now $v(a_6) \geq 3$. These cumulative translations imply $v(a_1) \geq 1$, $v(a_2) \geq 1$, $v(a_3) \geq 2$, $v(a_4) \geq 3$, and $v(a_6) \geq 3$. So by reducing $\frac{a_2}{\pi}$, $\frac{a_4}{\pi^2}$, and $\frac{a_6}{\pi^3} \pmod{\pi}$, we may form the polynomial in $\kappa[X]$:

$$F(X) = X^3 + \frac{a_2}{\pi} X^2 + \frac{a_4}{\pi^2} X + \frac{a_6}{\pi^3}. \tag{15}$$

    If $F(X)$ has distinct roots (or equivalently $v(a_2 a_4 + a_6) = 3$), then we are in the case $\boxed{I_0^*}$.

11. Otherwise $F(X)$ has multiple roots. Suppose that $F(X)$ has a double root and a single root, and that the double root is not rational over κ. Then $F(X)$ factors as $(X - \alpha)(X^2 - \beta)$ with β not a square in κ. This implies $v(a_4) = 2$, and $\beta = \frac{a_4}{\pi^2}$ is not a square in κ, so we may translate via $x \mapsto x' + \alpha\pi$, so that $v(a_2) \geq 2$, and $v(a_6) \geq 4$. Then we are in the case $\boxed{X_2}$.

12. Suppose instead that $F(X)$ has a double root and a single root, and that the double root is rational over κ. Then $F(X)$ factors as $(X - \alpha)\ (X - \beta)^2$. Now translate via $x = x' + \beta\pi$, and compute new $\{a_i\}$. The new $F(X)$ factors as $(X - \alpha')X^2$, with $\alpha' \neq 0$. Now $v(a_4) \geq 3$ and $v(a_6) \geq 4$, and $v(a_2) = 1$. We are therefore in one of the cases $\boxed{I_n^*}$, or $\boxed{T_n}$. We consult Table 7 to determine exactly which type it is.

13. If instead $F(X)$ has a triple root, $F(X)$ factors as $(X - \alpha)^3$ with $\alpha \in \kappa$. (A triple root of a cubic in characteristic 2 must always be rational.) Now translate via $x = x' + \alpha\pi$, and compute new $\{a_i\}$. The new $F(X)$ factors as X^3, so $v(a_4) \geq 3$, $v(a_6) \geq 4$, and $v(a_2) \geq 2$. Suppose additionally $v(a_3) = 2$. Then we are in the case $\boxed{IV^*}$.

14. If instead $v(a_3) \geq 3$ and $\frac{a_6}{\pi^4}$ is not a square in the residue field, then we are in the case $\boxed{Y_3}$.

15. If $\frac{a_6}{\pi^4}$ is a square in κ, translate via $y = y' + \alpha$ where $\alpha^2 = \frac{a_6}{\pi^4} \pmod{\pi}$ and compute new $\{a_i\}$. Now $v(a_6) \geq 5$. These cumulative translations imply $v(a_1) \geq 1$, $v(a_2) \geq 2$, $v(a_3) \geq 3$, $v(a_4) \geq 3$, and $v(a_6) \geq 5$. Suppose that additionally $v(a_4) = 3$. Then we are in the case $\boxed{III^*}$.

16. If instead $v(a_4) \geq 4$ and $v(a_6) = 5$, then we are in the case $\boxed{II^*}$.

17. If $v(a_6) \geq 6$, the cumulative conditions are $v(a_1) \geq 1, v(a_2) \geq 2, v(a_3) \geq 3, v(a_4) \geq 4$, and $v(a_6) \geq 6$. Then the Weierstrass equation is $\boxed{\text{Not Minimal}}$, so we replace the Weierstrass equation with a more minimal one via the transformation $a_i' = \frac{a_i}{\pi^i}$, and start over at step one.

The Weierstrass equation has been transformed into translated form, and the reduction type has been identified, unless the reduction type belongs to one of the families I_n, K_n, K_n', I_n^*, or T_n. In these cases, additional translations may be needed to put f into translated form and determine the exact reduction type.

5.2. Procedure for K_n Family

Even if an equation meets the conditions of the family K_n according to Table 5, it may still not be in fully translated form and in this case, the following procedure completes the translations and determines exactly which type it is.

1. Let $n = 1$.

2. If $v(a_6) = n$ then we have a type $\boxed{K_n}$.

3. Let $n = n + 1$.

4. If $v(b_8) = n$ then we have a type $\boxed{K_n}$.

5. If $Y^2 = a^2X^2 + a_6/\pi^n \pmod{\pi}$ has no rational points, then we have a type $\boxed{K_n'}$.

6. Let X_0 and Y_0 be two elements in R such that (X_0, Y_0) reduces to the rational point. Translate via $x = x + X_0\pi^{n/2}$ and $y = y + Y_0\pi^{n/2}$ so that $v(a_6) > n$.

7. Let $n = n + 1$.

8. Go to step number 2.

6. CONSTRUCTING REGULAR MODELS WITH BLOW-UPS

In order to complete the proof of Theorem 3.1 and to prove that the procedures described by Theorem 5.1 always serve as an algorithm to determine the reduction type, we need to verify that the conditions defined in section 4 are correct. The conditions associated to a particular type are correct if they imply that the sequence of blow-ups produces a special fiber of that type. Thus, explicit calculations of these blow-ups prove the following theorem. (In this section we denote a candidate reduction type with Ξ.)

THEOREM 6.1. *Let R be an arbitrary DVR with residue field κ. Let f be a minimal Weierstrass equation with coefficients in R, which is in translated form, meeting the conditions associated to a reduction type Ξ. Let E/K be the elliptic curve defined by f. Then there exists a sequence of blow-ups, (specified in [22, 24]), which produce a regular model C, whose generic fiber is E/K, and whose special fiber is of type Ξ.*

When κ is perfect, Theorem 6.1 is a restatement of Tate's algorithm. One case of this theorem, when κ is not perfect, is easy to prove. Namely, if the Weierstrass equation f satisfies the conditions of a standard reduction type, the usual blow-ups of Tate's algorithm still produce the regular model. By verifying this, one proves the lemma below. This proof amounts to a simple check that, for the standard reduction types, the translations requested by Tate's algorithm are all κ-rational.

LEMMA 1. *Let R be an arbitrary DVR, and let f be a minimal Weierstrass equation with coefficients in R, in translated form, meeting the conditions associated to a standard reduction type Ξ. Then the sequence of blow-ups specified in Tate's algorithm produces a regular model with the correct reduction type Ξ.*

The remaining ingredients needed to complete Theorem 6.1 are the case-by-case analyses for each new reduction type. For each of the new reduction types, following Tate's algorithm directly would entail making a non κ-rational translation.

Not being able to complete the sequence of blow-ups might seem to impede the resolution of singularities. However, terminating the sequence of blow-ups at this point already yields a regular scheme.

This implies that for each new reduction type, the required blow-ups follow the same sequence as for one of the standard types. The correspondence (16) below gives an example for each new reduction type of a standard type with the same sequence of blow-ups.

Z_1	Z_2	X_1	X_2	Y_1	Y_2	Y_3	K_{2n}	K'_{2n}	K_{2n+1}	T_n
I_0	I_0^*	I_0	I_0^*	I_0	IV	IV^*	I_{2n}	I_{2n}	I_{2n+1}	I_n^*

(16)

Having defined the sequence of blow-ups required for each new type, we should now verify that the resulting schemes are all regular. Intuitively, this is true because any would-be singularities are not κ-rational. We will now present complete details in two representative cases: type Z_1, and type Y_2.

6.1. Char 3 Z_1 Type

For our first example, will show that the conditions associated with Type Z_1 are correct (i.e. the special fiber is a cuspidal cubic). We begin with the subscheme of $R[x, y]$ defined by an equation satisfying the conditions in the column of Table 4 that is labeled Z_1. In other words, the cubic

$$y^2 = x^3 + a_2x^2 + a_4x + a_6 \tag{17}$$

satisfies $v(a_2) > 0$, $v(a_4) > 0$, $v(a_6) = 0$, and the requirement that a_6 is not a cube in κ.

We now look for singularities and perform a blow-up if any are found. By setting $\frac{df}{dy} = 0$, we find that any singular point must be contained in the subscheme defined by $\pi = 0$, $2y = 0$, and $x^3 + a_6 = 0$. Because $char(\kappa) = 3$, we know that $x^3 + a_6 = (x + \alpha)^3 \pmod{\pi}$ where $\alpha^3 = a_6$. Thus the x-coordinate of the cusp is the cube root of $a_6 \pmod{\pi}$, which is not κ-rational. Therefore the cusp does not correspond to a singular point of $\tilde{C}$.

More precisely, the image of the geometric cusp in $\tilde{C}$ is the point defined by the ideal $m = (\pi, y, x^3 + a_6)$. This ideal is maximal, and because the polynomial (17)

TABLE 8
Blowing up a Point on a Surface

Patch 1	$y = x\,y_1,$	$\pi = x\,\pi_1.$
Patch 2	$x = y\,x_1,$	$\pi = y\,\pi_1.$
Patch 3	$x = \pi\,x_1,$	$y = \pi\,y_1.$

is not zero (mod m^2), the vector space $\frac{m}{m^2}$ is two dimensional, and so this point is a regular point. In fact, because the scheme defined by the polynomial (17) was already regular, no blow-ups were required at all.

To summarize, the geometric special fiber $\overline{C}$ is a cuspidal cubic. However, $\tilde{C}$ is everywhere regular and the cusp is only defined in a degree three extension of κ. This phenomenon is only possible because in characteristic three, a cubic polynomial need not be separable.

6.2. Char 2 Y_2 Type

For our second example, we show that the conditions associated with Type Y_2 are correct (i.e. its special fiber consists of two components, as in Figure 4). This time, we begin with a subscheme of $R[x, y]$ defined by an equation satisfying the conditions in the column of Table 5 that is labeled Y_2. In other words, the cubic

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{18}$$

satisfies $v(a_1) \geq 1, v(a_2) \geq 1, v(a_3) \geq 2, v(a_4) \geq 2, v(a_6) = 2$, and the requirement that $\frac{a_6}{\pi^2}$ is not a square in κ.

As usual, we now look for singularities and perform a blow-up if any are found. By inspection, the geometric special fiber $\overline{C}$ is a cuspidal cubic curve. However, this time the cusp is κ-rational and located at $x = 0$, $y = 0$. This point, considered as a point of C/R, is defined by the ideal $m = (x, y, \pi)$. By checking that $dim(m/m^2) = 3$, we see that it is a singular point.

To resolve this singularity we blow-up C at the singular point. According to our definition of a blow-up, the revised scheme is the closure of the graph of the morphism to $P^2(R)$ given by the coordinates (x, y, π). To be explicit, each of the three affine coordinate patches is given by the change of variables in Table 8.

We focus on the third coordinate patch, which is the affine subscheme of $R[x_1, y_1]$ defined by

$$y_1^2 + a_1x_1y_1 + \frac{a_3}{\pi}y_1 = x_1^3\pi + a_2x_1^2 + \frac{a_4}{\pi}x_1 + \frac{a_6}{\pi^2}. \tag{19}$$

The portion of $\overline{C}$ visible in this coordinate patch is the multiplicity 2 curve defined by $y_1^2 = \frac{a_6}{\pi^2}$. Of course, this curve is only of multiplicity two because $char(\kappa) = 2$.

The image of this double line in $\tilde{C}$, however, is generically regular. This can be seen by viewing it as the product of two regular schemes: $Spec(\kappa[y_1]/(y_1^2 - \frac{a_6}{\pi^2}))$ and $Spec(\kappa[x_1])$. We know that the first factor is regular because the polynomial $y_1^2 - \frac{a_6}{\pi^2}$ is irreducible. If one examines the first coordinate patch of the blow-up, the original rational curve can be seen to intersect the double line transversally.

To summarize, the geometric special fiber consists of a rational curve intersecting a double line transversally, and the image of this double line in $\tilde{C}$ is regular. Our blow-up has explicitly constructed the reduction type Y_2, defined in section 3. The fact that κ is not perfect admits the possibility that a quadratic polynomial might not be separable.

This example is typical of the new reduction types in characteristic two: a singular point or curve is only defined in a degree two extension of κ. For the types requiring more than one blow-up, there may be many coordinate patches to keep track of.

7. CONCLUSIONS AND FURTHER WORK

This concludes our description of the new reduction types, the presentation of the extention to Tate's algorithm, and the construction of the regular model. We chose to center the discussion of the extended Tate's algorithm around the valuations of the Weierstrass coefficients because this description succinctly describes the geometry and rationality of the special fiber.

The tables in this paper describe useful, albeit non-canonical, forms of Weierstrass equations which reveal the special fiber type. The translated form of a Weierstrass equation is also appealing since it automatically suggests the sequence of blow-ups which will produce the regular minimal model.

For a particular choice of DVR R, (e.g $\mathbf{Z}[t]_{(2)}$), the algorithm may be easily implemented with a computer program, provided one has a procedure to check whether elements of κ are squares, or cubes, and whether or not the quadratic curves of the form (14) have any rational points.

7.1. Group Schemes and Néron Models

While the focus of this paper is the construction of regular models, it is natural to ask for a description of these models in terms of Group Schemes and Néron models. When κ is perfect, we know that the Néron model of an elliptic curve coincides with the smooth part of a flat proper regular minimal model of the curve. In fact, the following statement does not require the assumption that κ is perfect.

PROPOSITION 7.1.1. *Let R be an arbitrary DVR, let $K = frac(R)$, and let E/K be an elliptic curve. Let C be a flat proper regular minimal model of E/K, and let C_{sm}/R be the smooth part of C/R. Then C_{sm}/R is the Néron model of E/K.*

Essentially the same techniques used to prove this when κ is perfect [2, 22], apply more generally. The approach is to first show that the smooth part of the regular model is a group scheme, and then use the assumptions of minimality and smoothness to obtain the Néron mapping property. Because the accounts available in the literature assume that κ is perfect, Lorenzini and Liu have explicitly presented a proof in [15].

Proposition 7.1.1 implies that the regular models constructed in this paper yield Néron models once the singular points on the special fiber have been discarded. Focusing on the case when the special fiber is a new reduction type, we see that the special fiber of the Néron model, C_{sm}, has at most two components. The order of the component group is specified in the following table.

Z_1	Z_2	X_1	X_2	Y_1	Y_2	Y_3	K_{2n}	K'_{2n}	K_{2n+1}	T_n
1	1	1	2	1	1	1	2	1	1	2

(20)

While the minimality and smoothness of C_{sm} can be used to show that it is a group scheme, in our case this is also possible with direct calculations. This is not difficult since there are at most two components. Let W denote the smooth part of the elliptic scheme defined by a Weierstrass equation. If the special fiber of the Néron model has only a single component, then $W = C_{sm}$, and we check that it is a group scheme by examining the elliptic curve's addition formula. One then checks that the three projective coordinates of the addition map $C_{sm} \times C_{sm} \to C_{sm}$ are never simultaneously zero, and therefore the group law on E/K immediately makes C_{sm} into a group scheme.

The special fiber has two components only for reduction types X_2, K_{2n}, and T_n. In such a case there exists an R-valued point, P, which reduces to the cusp in W. Translating by P yields an automorphism of C_{sm} of order two. By using this translation to identify the generic fibers of two copies of W, a scheme isomorphic to C_{sm} is produced. With this simpler description, it is straightforward to extend the group law on E/K to a morphism, proving that C_{sm} is a group scheme.

7.2. Applications and Further Work

Elliptic Schemes The original motivation for this work was the study of elliptic schemes over higher dimensional base schemes. This work is presented in [23] where schemes of arbitrary dimension are considered, and an algorithm to construct a regular scheme is presented. In this context, most of the DVRs which appear have non-perfect residue fields, and new phenomenon occur due to the fact that the discriminant may not be irreducible in the local rings of the base. We showed that it is possible to always construct flat regular models over high dimensional bases when $char\kappa > 3$. For the other cases, it was still true that the algorithms always terminated in our experiments, yet this was not proved for every (regular) base scheme. It would be interesting to explore relationships with the general resolution of singularities [1], and the generalization which allows finite extentions[12].

Extentions and Representations A natural extention of this work is the study of how the reduction types change with finite extentions R'/R. Contrary to the perfect residue field case, the geometric special fiber of the regular model can change when an unramified extention of κ is made.

It is also natural to look for an appropriate definition of a conductor in the case when κ is not perfect. This would involve finding a good definition for the higher ramification groups needed to define the Swan representation. If a good definition can be made, can we find a relationship between the valuation of the conductor, discriminant, and number of components in the regular model? This would attempt to generalize Ogg's formula, treated by Ogg [19] when $char(\kappa) \neq 2$, and by Saito[20] in general. (Liu specializes this to elliptic curves in [14].) Ogg's formula is the commonly used tool to compute the exponent in the conductor of an elliptic curve when $char(\kappa) = 2$, or $char(\kappa) = 3$.

Component Pairings As described in the introduction, the new reduction types of section 3 have been applied to the study of the Grothendieck pairing on an elliptic curve. This map pairs a component of the special fiber of the Néron model with a component of the special fiber of the dual Néron model, and produces an element of $\mathbf{Q}/\mathbf{Z}$. Bertapelle, Bosch, and Lorenzini[3, 4, 5, 16] compared this pairing with the matrix of intersection multiplicities of the special fiber in a regular proper model of an elliptic curve or jacobian. With this new tool, they computed the Grothendieck pairing explicitly, discovering cases for which it is not perfect.

REFERENCES

[1] S. S. Abhyankar, Resolution of Singularities of Arithmetic Surfaces, Harper and Row, New York, 1965, 111-152.

[2] M. Artin, *Lipman's Proof of Resolution of Singularities* in Arithmetic Geometry, G. Cornell and J. Silverman, Eds, Springer-Verlag, 1986.

[3] A. Bertapell and S. Bosch, Weil Restriction and Grothendieck's Duality Conjecture, *J. Alg. Geom 9*, 2000, 155-164.

[4] S. Bosch and Q. Liu, Rational Points on the Group of Components of a Néron Model, *Manus. Math. 98*, 1999, 275-293.

[5] S. Bosch and D. Lorenzini, Grothendieck's Pairing On Component Groups of Jacobians, *Invent. Math. 148*, 2002, 353-396.

[6] J. Dieudonné and A. Grothendieck, Eléments de Géométrie Algébrique, *Publ, Math. IHES 24*, 1965, 1-231.

[7] D. Eisenbud, Commutative Algebra With a View Toward Algebraic Geometry, *Graduate Texts in Mathematics 150*, Springer-Verlag, 1995.

[8] D. Eisenbud and J. Harris, The Geometry of Schemes, *Graduate Texts in Mathematics 197*, Springer-Verlag, 2000.

[9] A. Grothendieck, Groupes de Monodromie en Géométrie Algébrique SGA 7 I, Springer-Verlag, 1972.

[10] R. Hartshorne, Algebraic Geometry, *Graduate Texts in Mathematics 52*, Springer-Verlag, 1977.

[11] H. Hironaka, Resolution of Singularities of an Algebraic Variety Over a Field of Characteristic Zero, *Annals of Math 79*, 1964, 109-326.

[12] A.J. de Jong, Smoothness, Semi-stability and Alterations, *Publ. Math. I.H.E.S. 83*, 1996, 51-93.

[13] K. Kodaira, On Compact Analytic Surfaces II, *Annals of Math*, vol. 77, 1963, 563-626.

[14] Q. Liu, Formule d'Ogg d'après Saito, Private Note.

[15] Q. Liu and D. Lorenzini, Néron Models of Elliptic Curves, Private Note, 2001.

[16] D. Lorenzini, Reduction in the Case of Imperfect Residue Fields, Preprint, 2001.

[17] R. Miranda, Smooth Models for Elliptic Threefolds in: R. Friedman, D.R. Morrison (Eds.), *The Birational Geometry of Degenerations*, *Progress in Mathematics 29*, Birkhauser, 1983, 85-133.

[18] A. Néron, Modèles Minimaux des Variétés Abéliennes sur les Corps Locaux et Globaux, *Publ. Math. I.H.E.S. 21*, 1964, 361-482.

[19] A. Ogg, Elliptic Curves and Wild Ramification, *Am. J. of Math 89*, 1967, 1-21.

[20] T. Saito, Conductor, Discriminant, and the Noether Formula of Arithmetic Surfaces, *Duke Math. J. 57*, 1988, 151-173.

[21] J. Silverman, The Arithmetic of Elliptic Curves, *Graduate Texts in Mathematics 106*, Springer-Verlag, 1991.

[22] J. Silverman, Advanced Topics in The Arithmetic of Elliptic Curves, *Graduate Texts in Mathematics 151*, Springer-Verlag, 1996.

[23] M. Szydlo, Flat Regular Models of Elliptic Schemes, Ph.D thesis, Harvard University, 1999.

[24] J. Tate, Algorithm for Determining the Type of a Singular Fiber in an Elliptic Pencil, *Modular Functions of One Variable IV*, Lecture Notes in Math 476, Springer-Verlag, 1975, 33-52.